Symmetric powers and modular invariants of elementary abelian p-groups

Jonathan Elmer

PII: S0021-8693(17)30426-X
DOI: http://dx.doi.org/10.1016/j.jalgebra.2017.07.020
Reference: YJABR 16323

To appear in: *Journal of Algebra*

Received date: 23 March 2017

Please cite this article in press as: J. Elmer, Symmetric powers and modular invariants of elementary abelian p-groups, *J. Algebra* (2017), http://dx.doi.org/10.1016/j.jalgebra.2017.07.020

SYMMETRIC POWERS AND MODULAR INVARIANTS OF ELEMENTARY ABELIAN p-GROUPS

JONATHAN ELMER

Abstract. Let E be a elementary abelian p-group of order $q = p^n$. Let W be a faithful indecomposable representation of E with dimension 2 over a field $\Bbbk$ of characteristic p, and let $V = S^m(W)$ with $m < q$. We prove that the rings of invariants $\Bbbk[V]^E$ are generated by elements of degree $\leq q$ and relative transfers. This extends recent work of Wehlau [18] on modular invariants of cyclic groups of order p. If $m < p$ we prove that $\Bbbk[V]^E$ is generated by invariants of degree $\leq 2q-3$, extending a result of Fleischmann, Sezer, Shank and Woodcock [6] for cyclic groups of order p . Our methods are primarily representation-theoretic, and along the way we prove that for any $d < q$ with $d + m \geq q$, $S^d(V^*)$ is projective relative to the set of subgroups of E with order $\leq m$, and that the sequence $S^d(V^*)_{d\geq 0}$ is periodic with period q, modulo summands which are projective relative to the same set of subgroups. These results extend results of Almkvist and Fossum [1] on cyclic groups of prime order.

1. Introduction

1.1. **Modular invariant theory and degree bounds.** Let G be a finite group and $\Bbbk$ a field of arbitrary characteristic. Let V be a finite-dimensional representation of G, which in this article will always mean a left $\Bbbk G$-module. We denote by $\Bbbk[V]$ the $\Bbbk$-algebra of polynomial functions $V \to \Bbbk$. This itself becomes a $\Bbbk G$-module with the action given by

$$(\sigma f)(v) = f(\sigma^{-1}v)$$

for $f \in \Bbbk[V], v \in V$ and $\sigma \in G$.

Let $\{x_1, x_2, \ldots, x_n\}$ be a basis for V^*. If $\Bbbk$ is infinite, we can identify $\Bbbk[V]$ with the polynomial ring $\Bbbk[x_1, x_2, \ldots, x_n]$; this is graded by total degree, and the action of G on $\Bbbk[x_1, x_2, \ldots, x_n]$ is by graded algebra automorphisms. As a $\Bbbk G$-module, the homogeneous component of degree d in $\Bbbk[V]$ is isomorphic to $S^d(V^*)$, the dth symmetric power of V^*.

The set of fixed points $\Bbbk[V]^G$ forms a $\Bbbk$-subalgebra of $\Bbbk[V]$ called the *algebra of invariants*. This is the central object of study in invariant theory. The most natural goal in invariant theory is to compute algebra generators of $\Bbbk[V]^G$. This is a hard problem in general, especially if $|G|$ is divisible by $\Bbbk$. For example, even for cyclic groups of order p the list of modular representations V for which algebra generators of $\Bbbk[V]^G$ are known is rather short, see [18]. Some general results are known, however. Famously, Noether proved that the ring of invariants $\mathbb{C}[V]^G$ has a generating set consisting of invariants of degree $\leq |G|$, for any representation of G over $\mathbb{C}$. For this reason, the minimum d such that $\oplus_{i=0}^d \Bbbk[V]_i^G$ generates $\Bbbk[V]^G$ as a $\Bbbk$-algebra is called the *Noether bound* and written as $\beta(\Bbbk[V]^G)$. Her results were extended independently by Fleischmann [8] and Fogarty [9] to any field whose characteristic does not divide the order of G, the so called non-modular case. In

Date: August 3, 2017.

2010 *Mathematics Subject Classification.* 20C20, 13A50.

Key words and phrases. modular representation theory, invariant theory, elementary abelian p-groups, symmetric powers, relative stable module category.

contrast, it is known that in the modular case no general bound on the degrees of generators which depends on $|G|$ alone exists. Recent work of Symonds [15] has shown that, independently of the characteristic of $\Bbbk$, $\Bbbk[V]^G$ is generated by invariants of degree at most $\max(|G|, (|G|-1)\dim(V))$.

Fleischmann, Sezer, Shank and Woodcock [6] proved that if V is an indecomposable modular representation of a cyclic group of order p, then $\Bbbk[V]^G$ is generated by invariants of degree at most $2p-3$. In particular this shows that Symonds' bound is far from sharp. One goal of this article is to prove the following result:

Theorem 1.1. *Let E be an elementary abelian p-group of order q, $\Bbbk$ an infinite field of characteristic p, W a faithful indecomposable $\Bbbk E$-module with dimension 2. Let $V = S^m(W)$ with $m < p$. Then $\Bbbk[V]^E$ is generated by invariants of degree $\leq 2q-3$.*

Note that if $E = C_p$ is a cyclic group of order p there is only one isomorphism class of faithful indecomposable representation of dimension 2. Furthermore, if V is any indecomposable $\Bbbk C_p$-module then $V = S^m(W)$ for some $m < p$. So the above generalises [6, Proposition 1.1(a)].

1.2. **The transfer.** Let G be a finite group, $H \leq G$ and M a $\Bbbk G$-module. We denote the set of G-fixed points in M by M^G. There is a $\Bbbk G$-map $M^H \to M^G$ defined as follows:

$$Tr_H^G(f) = \sum_{\sigma \in S} \sigma f$$

where $f \in M$ and S is a left-transversal of H in G. This is called the relative trace or transfer. It is clear that the map is independent of the choice of S. If $H = 1$ we usually write this as Tr^G and call it simply the trace or transfer.

In case $M = \Bbbk[V]$ this restricts to a degree-preserving $\Bbbk[V]^G$-homomorphism $\Bbbk[V]^H \to \Bbbk[V]^G$, whose image is an ideal of $\Bbbk[V]^G$. We denote its image by I_H^G . More generally, given a set $\mathcal{X}$ of subgroups of G, we set $I_{\mathcal{X}}^G = \sum_{H \in \mathcal{X}} I_H^G$.

If $|G : H|$ is not divisible by $\mathrm{char}(\Bbbk)$ then Tr_H^G is surjective. This has many nice consequences; in particular, it implies that $\Bbbk[V]^G$ is a direct summand of $\Bbbk[V]^H$ as a $\Bbbk[V]^G$-module, and hence that $\Bbbk[V]^G$ is Cohen-Macaulay if $\Bbbk[V]^H$ is. It also shows that in the non-modular case, every invariant lies in the image of the transfer map and every ring of invariants is Cohen-Macaulay.

From now on suppose that G is divisible by $p = \mathrm{char}(\Bbbk) > 0$. Choose a Sylow-$p$-subgroup P of G and denote by $I_{<P}^G$ the sum of all I_Q^G with $Q < P$. It is easily shown that $I_{<P}^G$ is independent of the choice of P. The ring $\Bbbk[V]^G/I_{<P}^G$ has attracted some attention in recent years. The prevailing idea is that it behaves in many ways like a non-modular ring of invariants. For example, Totaro [16] has shown that $\Bbbk[V]^G/I_{<P}^G$ is a Cohen-Macaulay ring for any G and V, generalising earlier work of Fleischmann [7], where $I_{<P}^G$ is replaced by its radical. In the same spirit is the following conjecture, reported by Wehlau [17].

Conjecture 1.2. *Let G be a finite group and V a $\Bbbk G$-module. Then $\Bbbk[V]^G/I_{<P}^G$ is generated by invariants of degree $\leq |G|$.*

It had earlier been shown that this holds whenever V is an indecomposable representation of a cyclic group of order p. In the present article we prove

Theorem 1.3. *Let E be an elementary abelian p-group of order q, $\Bbbk$ an infinite field of characteristic p, W a faithful indecomposable $\Bbbk E$-module with dimension 2. Let $V = S^m(W)$ with $m < q$. Then $\Bbbk[V]^E/I_{<E}^E$ is generated by invariants of degree $\leq q$.*

In other words, this class of representations of elementary abelian p-groups satisfies Conjecture 1.2. Once more, as every indecomposable representation of a cyclic group can be written as a symmetric power of the unique indecomposable representation of degree 2, this is a generalisation of the earlier result.

1.3. **Symmetric powers and relative projectivity.** Let G be a finite group and let V and W be finite-dimensional representations of G over a field $\Bbbk$. Let $v_1, v_2, \dots, v_m$ and $w_1, w_2, \dots, w_n$ be bases of V and W over $\Bbbk$. Then the tensor product $V \otimes W$ of V and W is the $\Bbbk$-vector space spanned by elements of the form $v_i \otimes w_j$, where scalar multiplication satisfies $\lambda(v_i \otimes w_j) = (\lambda v_i) \otimes w_j = v_i \otimes (\lambda w_j)$ for all $\lambda \in \Bbbk$. There is a linear action of G on the space defined by $g(v_i \otimes w_j) = gv_i \otimes gw_j$. We can take the tensor product of V with itself, and iterate the construction d times to obtain, for any natural number d, a module $T^d(V) = V \otimes \cdots \otimes V$, called the *dth tensor power* of V. Formally, the dth *symmetric power* $S^d(V)$ of V is defined to be the quotient of $T^d(V)$ by the subspace generated by elements of the form $v_1 \otimes \cdots \otimes v_d - v_{\sigma(1)} \otimes \ldots \otimes v_{\sigma(d)}$ where $\sigma \in \Sigma_d$, the symmetric group on $\{1, 2, \dots, d\}$. We have $S^0(V) \cong \Bbbk$ for any V, and we use the convention that $S^d(V) = 0$ for negative values of d.

Symmetric powers of indecomposable representations are not indecomposable in general, and a central problem in representation theory is to try to understand their indecomposable summands. If $|G|$ is invertible in $\Bbbk$ then this is largely a matter of character theory. The first authors to consider the problem in the modular case were Almkvist and Fossum [1]. In this remarkable work, the authors give formulae for the indecomposable summands of any representation of the form $V \otimes W$, $S^d(V)$ or $\Lambda^d(V)$ (exterior power), where V and W are indecomposable representations of a cyclic group of order p over a field $\Bbbk$ of characteristic p. Some of these formulae were generalised to the case of finite groups whose Sylow-p-subgroup is cyclic by Hughes and Kemper [11], and to cyclic 2-groups in [10].

Now let $H \leq G$ and let M be a $\Bbbk H$-module. Then $\Bbbk G \otimes_{\Bbbk H} M$ is naturally a $\Bbbk G$-module, which we call the $\Bbbk G$-module *induced* from M, and write as $M \uparrow_H^G$. When $\alpha : M \to N$ is a $\Bbbk H$-homomorphism we define $\alpha \uparrow_H^G \colon M \uparrow_H^G \to N \uparrow_H^G$ by $\alpha \uparrow_H^G := \mathrm{id}_{\Bbbk G} \otimes_{\Bbbk H} \alpha$.

A $\Bbbk G$-module M which is a direct summand of $M \downarrow_H \uparrow_H^G$ is said to be projective relative to H, or simply projective if $H = 1$. Other equivalent definitions will be given in Section 2. More generally, for a set $\mathcal{X}$ of subgroups of G, a $\Bbbk G$-module M is said to be projective relative to $\mathcal{X}$ if it is a direct summand of $\oplus_{X \in \mathcal{X}} M \downarrow_X \uparrow_X^G$.

We will also show in section 2 that if M is projective relative to $\mathcal{X}$ then $M^G = \sum_{X \in \mathcal{X}} \mathrm{Tr}_X^G(M^X)$. Consequently, invariants in $\Bbbk[V]^G$ which lie in summands of $\Bbbk[V]$ which are projective relative to $\mathcal{X}$ are contained in $I_{\mathcal{X}}^G$.

The following results of Almkvist and Fossum concerning representations of cyclic groups of prime order are of particular interest to us.

Theorem 1.4 (Almkvist and Fossum)**.** *Let $G = C_p$ be a cyclic group of prime order p and let $\Bbbk$ be a field of characteristic p. Let V be the unique indecomposable representation of G over $\Bbbk$ with dimension 2 (with action given by a Jordan block of size two).*

(i) *(Projectivity) Suppose $m, d < p$ and $m + d \geq p$. Then $S^d(S^m(V))$ is projective.*

(ii) *(Periodicity) For any $m, d < p$ and any r we have a $\Bbbk G$-isomorphism $S^{pr+d}(S^m(V)) \cong S^d(S^m(V)) +$ projective modules.*

Of course, in determining the indecomposable summands of any modular representation of C_p, one is helped enormously by the fact that we have a classification of indecomposable representations. Indeed, the modules $V_{d+1} := S^d(V)$ for $0 \leq d < p$,

form a complete set of isomorphism classes of indecomposable modular representations for C_p, and V_p is the unique projective indecomposable. Furthermore, each has a C_p-fixed subspace of dimension 1, and so the number of indecomposable summands in a given representation is equal to the dimension of the subspace fixed by C_p. For representations of elementary abelian p-groups, neither of these helpful results hold. In fact, if G is an elementary abelian p-group of order p^n, then unless $n = 1$ or $p = n = 2$, the representation type of G is "wild"; essentially this means that there is no hope of classifying the indecomposable representations up to isomorphism. In spite of this, we prove the following:

Theorem 1.5. *Let E be an elementary abelian p-group of order q, $\Bbbk$ a field of characteristic p and V a faithful indecomposable $\Bbbk E$-module with dimension 2. Let $m, d < q$ with $m + d \geq q$. Then $S^d(S^m(V)^*)$ is projective relative to the set of subgroups of E with order $\leq m$.*

Note that in case E is cyclic of order p, $S^m(V)$ is self-dual, so this generalises the first part of Theorem 1.4. We also prove the following generalisation of the second part:

Theorem 1.6. *Retain the notation of Theorem 1.5. Let m, d be integers with $m < q$, $d > q$ and let $d' \equiv d \mod q$ with $0 \leq d' < q$. Then $S^d(S^m(V)^*) \cong S^{d'}(S^m(V)^*)$ modulo summands which are projective relative to the set of subgroups of E with order $\leq m$.*

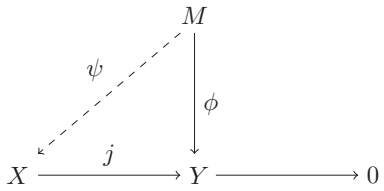
1.4. **Structure of the paper.** In order to prove results like the two theorems above, we need to determine the isomorphism type of $\Bbbk G$-modules up to the addition of other $\Bbbk G$-modules which are projective relative to certain families of subgroups. Given any set $\mathcal{X}$ of subgroups of G, one can define a category whose objects can be viewed as residue classes of $\Bbbk G$-modules up to the addition of relatively $\mathcal{X}$-projective modules. This is called the $\mathcal{X}$-relative stable module category. In case $\mathcal{X} = \{1\}$ it reduces to the stable module category, which has been written about extensively by many authors. We recommend [4] as a good reference. Many familiar results about the stable module category generalise in a straightforward manner. In section 2 we define the $\mathcal{X}$-relative stable module category and gather together the results we need, in most cases omitting proofs. The goal of the section is to prove a result (Corollary 2.7) which says something about the relationship between stable module categories relative to different families of subgroups.

The main body of work in this paper is section 3, in which we prove Theorems 1.5 and 1.6. In section 4 we turn our focus to invariant theory, in particular proving Theorems 1.1 and 1.3.

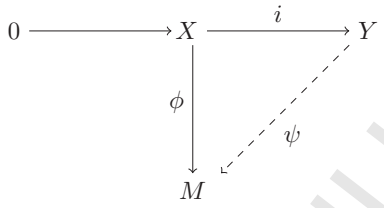
Acknowledgments. Special thanks go to Professor David Benson a number of invaluable conversations at the genesis of this work. Thanks also to Dr. Müfit Sezer for his assistance with the proof of Proposition 4.3, and an anonymous referee for some helpful remarks.

2. Relative projectivity and the relative stable module category

In this section, we fix a prime $p > 0$ and let G be a finite group of order divisible by p. Let $\Bbbk$ be a field of characteristic p and let $\mathcal{X}$ be a set of subgroups of G. Now let M be a finitely generated $\Bbbk G$-module. M is said to be *projective relative to* $\mathcal{X}$ if the following holds: let $\phi : M \to Y$ be a $\Bbbk G$-homomorphism and $j : X \to Y$ a surjective $\Bbbk G$-homomorphism which splits on restriction to any subgroup of $H \in \mathcal{X}$. Then there exists a $\Bbbk G$-homomorphism ψ making the following diagram commute.



Dually, one says that M is *injective relative to* $\mathcal{X}$ if the following holds: given an injective $\Bbbk G$-homomorphism $i : X \to Y$ which splits on restriction to each $H \in \mathcal{X}$ and a $\Bbbk G$-homomorphism $\phi : X \to M$, there exists a $\Bbbk G$-homomorphism ψ making the following diagram commute.



These notions are equivalent to the usual definitions of projective and injective $\Bbbk G$-modules when we take $\mathcal{X} = \{1\}$. We will say a $\Bbbk G$-homomorphism is $\mathcal{X}$-split if it splits on restriction to each $H \in \mathcal{X}$. Since a $\Bbbk G$-module is projective relative to H if and only if it is also projective relative to the set of all subgroups of H, we usually assume $\mathcal{X}$ is closed under taking subgroups.

Relative projectivity is associated very closely with the transfer maps defined in subsection 1.2. Given $\Bbbk G$-modules and M and N, there is a natural left action of G on $\mathrm{Hom}_{\Bbbk}(M, N)$ defined by

$$(\sigma \cdot \alpha)v = \sigma\alpha(\sigma^{-1}v), \qquad \sigma \in G, \alpha \in \mathrm{Hom}_{\Bbbk}(M, N), v \in M.$$

We write (M, N) for $\mathrm{Hom}_{\Bbbk}(M, N)$, so that $(M, N)^G = \mathrm{Hom}_{\Bbbk G}(M, N)$. If H is a subgroup of G, then the map $\mathrm{Tr}_H^G : (M, N)^H \to (M, N)^G$ will be defined as

$$\mathrm{Tr}_H^G(\alpha)(v) = \sum_{\sigma \in S} \sigma\alpha(\sigma^{-1}v).$$

There is also a map $\mathrm{res}_H^G : (M, N)^G \to (M, N)^H$ obtained by restricting homomorphisms. We note the following properties of transfer:

Lemma 2.1. (1) *Let $\alpha \in (M, N)^H$ and $\beta \in (M, M)^G$. Then $\mathrm{Tr}_H^G(\alpha) \circ \beta = \mathrm{Tr}(\alpha \circ \mathrm{res}_H^G(\beta))$.*

(2) *Let $\alpha \in (N, N)^G$ and $\beta \in (M, N)^H$. Then $\alpha \circ \mathrm{Tr}_H^G(\beta) = \mathrm{Tr}(\mathrm{res}_H^G(\alpha) \circ \beta)$.*

Proof. See [2, Lemma 3.6.3(i), (ii)]. □

There are many equivalent ways to characteristic relative projectivity:

Proposition 2.2. *Let G be a finite group of order divisible by p, $\mathcal{X}$ a set of subgroups of G and M a $\Bbbk G$-module. Then the following are equivalent:*

(i) *M is projective relative to $\mathcal{X}$;*
(ii) *Every $\mathcal{X}$-split epimorphism of $\Bbbk G$-modules $\phi : N \to M$ splits;*
(iii) *M is injective relative to $\mathcal{X}$;*
(iv) *Every $\mathcal{X}$-split monomorphism of $\Bbbk G$-modules $\phi : M \to N$ splits;*
(v) *M is a direct summand of $\oplus_{H \in \mathcal{X}} M{\downarrow_H}{\uparrow^G}$;*
(vi) *M is a direct summand of a direct sum of modules induced from subgroups in $\mathcal{X}$*

(vii) *There exists a set of homomorphisms* $\{\beta_H : H \in \mathcal{X}\}$ *such that* $\beta_H \in (M,M)^H$ *and* $\sum_{H\in\mathcal{X}} \mathrm{Tr}_H^G(\beta_H) = \mathrm{Id}_M$.

The last of these is called *Higman's criterion*.

Proof. The proof when $\mathcal{X}$ consists of a single subgroup of G can be found in [2, Proposition 3.6.4]. This can easily be generalised. □

Note that (vi) tells us that M is projective relative to $\mathcal{X}$ if and only if M decomposes as a direct sum of modules, each of which is projective to some single $H \in \mathcal{X}$. The following corollary now follows immediately from [2, Corollary 3.6.7].

Corollary 2.3. *Suppose* M *and* N *are* $\Bbbk G$*-modules and* N *is projective relative to* $\mathcal{X}$. *Then* $M \otimes N$ *is projective relative to* $\mathcal{X}$.

Let M and N be $\Bbbk G$-modules and let $\mathcal{X}$ be a set of subgroups of G. Let $(M,N)^{G,\mathcal{X}}$ denote the linear subspace of $(M,N)^G$ consisting of homomorphisms which factor through some $\Bbbk G$-module which is projective relative to $\mathcal{X}$. We consider the quotient

$$(M,N)^G_{\mathcal{X}} = (M,N)^G/(M,N)^{G,\mathcal{X}}.$$

One can define a category in which the objects are the $\Bbbk G$-modules and $(M,N)^G_{\mathcal{X}}$ is the set of morphisms between $\Bbbk G$-modules M and N. This is called the $\mathcal{X}$-relative stable module category, or ${}_{\mathcal{X}}\mathrm{stmod}_{\Bbbk G}$ for short. It reduces to the usual stable module category when we take $\mathcal{X} = \{1\}$.

The question of whether a homomorphism factors through a relatively projective module is also related to the transfer.

Lemma 2.4. *Let* M, N *be* $\Bbbk G$*-modules,* $\mathcal{X}$ *a collection of subgroups of* G, *and* $\alpha \in (M,N)^G$. *Then the following are equivalent:*

(1) α *factors through* $\oplus_{H\in\mathcal{X}} M{\downarrow_H}{\uparrow^G}$.
(2) α *factors through some module which is projective relative to* $\mathcal{X}$.
(3) *There exist homomorphisms* $\{\beta_H \in (M,N)^H : H \in \mathcal{X}\}$ *such that* $\alpha = \sum_{H\in\mathcal{X}} \mathrm{Tr}_H^G(\beta_H)$.

Proof. This is easily deduced from [2, Proposition 3.6.6]. □

If $\alpha, \beta \in (M,N)^G$, we will write $\alpha \equiv_{\mathcal{X}} \beta$ whenever α and β are equivalent as morphisms in ${}_{\mathcal{X}}\mathrm{stmod}_{\Bbbk G}$. In other words, whenever $\alpha - \beta \in \oplus_{X\in\mathcal{X}} \mathrm{Tr}_X^G(M,N)^X$. A homomorphism $\alpha \in (M,N)^G$ induces an isomorphism in ${}_{\mathcal{X}}\mathrm{stmod}_{\Bbbk G}$ if and only if there exists a homomorphism $\beta \in (N,M)^G$ with the property that $\alpha\circ\beta \equiv_{\mathcal{X}} \mathrm{id}_N$ and $\beta\circ\alpha \equiv_{\mathcal{X}} \mathrm{id}_M$. We shall write $M \simeq_{\mathcal{X}} N$ to say that M and N are isomorphic as objects in ${}_{\mathcal{X}}\mathrm{stmod}_{\Bbbk G}$. The following is now easy to deduce:

Lemma 2.5. *Let* M *and* N *be* $\Bbbk G$*-modules. Then the following are equivalent:*

(1) $M \simeq_{\mathcal{X}} N$;
(2) *There exist* $\Bbbk G$*-modules* P *and* Q *which are projective relative to* $\mathcal{X}$ *such that* $M \oplus P \cong N \oplus Q$.

The next result, which we will need in the proof of our main theorem, is a generalisation of [14, Lemma 3.1].

Proposition 2.6. *Let* G *be a finite group,* $\mathcal{X}$ *a set of subgroups of* G *which is closed under taking subgroups, and* $\mathcal{Y}$ *a non-empty subset of* $\mathcal{X}$. *Let* M *and* N *be* $\Bbbk G$*-modules and suppose that either* M *or* N *is projective relative to* $\mathcal{X}$. *Suppose* $\alpha \in (M,N)^G$ *has the property that* $\mathrm{res}_H^G(\alpha)$ *factors through a module which is projective relative to the set* $H \cap \mathcal{Y} := \{K \in \mathcal{Y} : K \subseteq H\}$, *for every* $H \in \mathcal{X}$. *Then* α *factors through a module which is projective relative to* $\mathcal{Y}$.

Proof. We give the proof when M is projective relative to $\mathcal{X}$; the proof when N is projective relative to $\mathcal{X}$ is similar. By Lemma 2.4, we can write, for each $H \in \mathcal{X}$

$$\mathrm{res}^G_H(\alpha) = \sum_{K \in H \cap \mathcal{Y}} \mathrm{Tr}^H_K(\beta_{H,K})$$

where $\beta_{H,K} \in (M,N)^K$. Since M is projective relative to $\mathcal{X}$ we can write

$$\mathrm{Id}_M = \sum_{H \in \mathcal{X}} \mathrm{Tr}^G_H(\mu_H)$$

for some set of homomorphisms $\{\mu_H \in (M,M)^H : H \in \mathcal{X}\}$. Now we have

$$\begin{aligned}\alpha = \alpha \circ Id_M &= \alpha \circ (\sum_{H \in \mathcal{X}} \mathrm{Tr}^G_H(\mu_H)) \\ &= \sum_{H \in \mathcal{X}} \mathrm{Tr}^G_H(\mathrm{res}^G_H(\alpha) \circ \mu_H)\end{aligned}$$

by Lemma 2.1(2),

$$\begin{aligned}&= \sum_{H \in \mathcal{X}} \mathrm{Tr}^G_H(\sum_{K \in H \cap \mathcal{Y}} \mathrm{Tr}^H_K(\beta_{H,K}) \circ \mu_H) \\ &= \sum_{H \in \mathcal{X}} \mathrm{Tr}^G_H(\sum_{K \in H \cap \mathcal{Y}} \mathrm{Tr}^H_K(\beta_{H,K} \circ \mathrm{res}^H_K(\mu_H)) \\ &= \sum_{H \in \mathcal{X}} (\sum_{K \in H \cap \mathcal{Y}} \mathrm{Tr}^G_K(\beta_{H,K} \circ \mathrm{res}^H_K(\mu_H)) \in (M,N)^{G,\mathcal{Y}}\end{aligned}$$

as required. □

Corollary 2.7. *Let $\alpha, \beta \in (M,N)^G$. Suppose that, for all $H \in \mathcal{X}$, $\mathrm{res}^G_H(\alpha) \equiv_{H \cap \mathcal{Y}} \mathrm{res}^G_H(\beta)$. Then $\alpha \equiv_{\mathcal{Y}} \beta$.*

Proof. Apply Proposition 2.6 to $\alpha - \beta$. □

Given any $\Bbbk G$-module M, it can be shown that there exists a surjective map $j : P \to M$, where P is a relatively $\mathcal{X}$-projective $\Bbbk G$-module and j splits on restriction to each $H \in \mathcal{X}$. The minimal such P is called the relatively $\mathcal{X}$-projective cover of M. This implies the existence, for any $\Bbbk G$-module M, of a unique minimal resolution $P_* \to M$ by relatively $\mathcal{X}$-projective modules which splits on restriction to each $H \in \mathcal{X}$. One can then show, using an argument along the lines of [4, Proposition 5.2] that a pair of maps $\alpha, \beta \in (M,N)^G$ satisfy $\alpha \equiv_{\mathcal{X}} \beta$ if and only if the maps α_* and β_* induced between minimal relatively $\mathcal{X}$-projective resolutions of M and N are chain homotopic. Dually, there exists an injective map $i : M \to Q$ where Q is a relatively $\mathcal{X}$-projective $\Bbbk G$-module and i splits on restriction to each $H \in \mathcal{X}$. The minimal such Q is called the relatively $\mathcal{X}$-injective hull of M, and leads to an analogous theory of minimal relatively $\mathcal{X}$-injective resolutions.

The categories ${}_{\mathcal{X}}\,\mathrm{stmod}_{\Bbbk G}$ are not abelian categories; kernels and cokernels of morphisms are not well-defined. Rather, they are triangulated category. See [13] for a full definition of a triangulated category. In a triangulated category there is a construction called a mapping cone, which replaces the cokernel. In ${}_{\mathcal{X}}\,\mathrm{stmod}_{\Bbbk G}$ this works as follows: given any morphism $M \to N$ we choose a representative $\alpha \in (M,N)^G$. Now let $j : \ker(\alpha) \to M$ be the canonical inclusion and denote by $i : \ker(\alpha) \to Q$ the inclusion into the relatively $\mathcal{X}$-injective hull of $\ker(\alpha)$. Since i splits on restriction to each $H \in \mathcal{X}$ there exists a $\theta \in (M,Q)^G$ such that $\theta \circ j = i$. Now define $\alpha' : M \to N \oplus Q$ by $\alpha'(m) = (\alpha(m), \theta(m))$. One can check that α' is injective. Then the mapping cone of the original morphism is defined to be the cokernel of α'. It can be shown in the fashion of [4, Proposition 5.5] (using the chain homotopy property of equivalent morphisms) that this construction is independent of the choice of α. Of course, if α is injective one can take $\alpha = \alpha'$. This implies

Lemma 2.8. *Let $\alpha, \beta \in (M,N)^G$ with $\alpha \equiv_{\mathcal{X}} \beta$. Suppose α and β are injective. Then* $\mathrm{coker}(\alpha) \simeq_{\mathcal{X}} \mathrm{coker}(\beta)$.

We end this section with an elementary result which will be useful in section 4.

Lemma 2.9. *Let M be a $\Bbbk G$-module which is projective relative to a set $\mathcal{X}$ of subgroups of G. Then $M^G = \sum_{H\in\mathcal{X}} \mathrm{Tr}_H^G(M^H)$.*

Proof. It suffices to prove $M^G \subseteq \sum_{H\in\mathcal{X}} \mathrm{Tr}_H^G(M^H)$, the reverse inclusion being clear. As M is projective relative to $\mathcal{X}$, there exists a set of homomorphisms $\{\beta_H \in (M,M)^H, H \in \mathcal{X}\}$ such that $\mathrm{Id}_M = \sum_{H\in\mathcal{X}} \mathrm{Tr}_H^G(\beta_H)$. Now let $v \in M^G$. As $v \in M^H$ for all $H \in \mathcal{X}$, we have $\beta_H(v) \in M^H$ for all $H \in \mathcal{X}$, and

$$\mathrm{Tr}_H^G(\beta_H)(v) = \sum_{\sigma\in S} \sigma\beta_H(\sigma^{-1}v) = \sum_{\sigma\in S} \sigma\beta_H(v) = \mathrm{Tr}_H^G(\beta_H(v))$$

where S is a left-transversal of H in G. Therefore

$$v = \mathrm{Id}_M(v) = \sum_{H\in\mathcal{X}} \mathrm{Tr}_H^G(\beta_H)(v) = \sum_{H\in\mathcal{X}} \mathrm{Tr}_H^G(\beta_H(v)) \in \sum_{H\in\mathcal{X}} \mathrm{Tr}_H^G(M^H)$$

as required. □

3. Decomposing Symmetric Powers

3.1. **Periodicity.** We begin by describing a decomposition of symmetric powers applicable to all p-groups. Let G be any finite p-group, $\Bbbk$ a field of characteristic p, and let V be any finite-dimensional indecomposable $\Bbbk G$-module. It is well-known that one may choose a basis $\{x_0, x_1, \ldots, x_m\}$ with respect to which the action of G is lower-unitriangular, preserving the flag of subspaces $\langle x_m\rangle \subset \langle x_{m-1}, x_m\rangle \subset \ldots \subset \langle x_0, x_1, \ldots, x_m\rangle$. We will refer to x_0 as the "terminal" variable and to x_m as the "initial" variable. For any $x \in V$ we set

$$N_G(x) = \prod_{y\in Gx} y$$

where Gx denotes the orbit of x under G.

Now let q denote the order of G, and let $B(V)$ be the set of all polynomials in $x_0, x_1, \ldots, x_m$ whose degree as a polynomial in x_0 alone is strictly less than q. $B(V) = \bigoplus_{d\geq 0} B^d(V)$ is graded by total degree. Since G fixes the subspace $\langle x_1, x_2, \ldots, x_m\rangle$, $B(V)$ is a $\Bbbk G$-submodule of $S(V)$. Further, given any $f \in S^d(V)$ with x_0-degree $\geq q$ we may perform long division, writing uniquely $f = N_G(x_0)^a f' + b$ with $f' \in S(V)^{d-q}$ and $b \in B(V)$, where $a = q/|Gx_0|$. We therefore obtain an isomorphism of graded $\Bbbk G$-modules

$$S(V)^d \cong N_G(x_0)^a \otimes S(V)^{d-q} \oplus B^d(V). \tag{1}$$

Remark 3.1. Suppose W is a direct summand of $S^d(V)$, and $f \in S^r(V)^G$. Then $f \otimes W$ is a submodule of $S^{d+r}(V)$ in general. One way of viewing the above is to say that $N_G(x_0) \otimes W$ is always a direct summand of $S^{d+q}(V)$. We sometimes say that W is *propagated* by the invariant $N_G(x_0)$. Note that if W is projective, then since projective modules are injective we have that $f \otimes W$ is a direct summand of $S^{d+r}(V)$ for any $f \in S^r(V)^G$ - in other words, the projective direct summands are propagated by every invariant.

Now since multiplication with x_m induces an injective map $S^d(V) \to S^{d+1}(V)$, there is an exact sequence of $\Bbbk G$-modules

$$0 \longrightarrow S^d(V) \xrightarrow{\times x_m} S^{d+1}(V) \longrightarrow S^{d+1}(V/x_m) \longrightarrow 0.$$

As multiplication by x_m does not affect the x_0-degree and the second map does not increase it, this restricts to an exact sequence of $\Bbbk G$-modules

$$0 \longrightarrow B^d(V) \xrightarrow{\alpha_d} B^{d+1}(V) \longrightarrow B^{d+1}(V/x_m) \longrightarrow 0.$$

3.2. **Additive subgroups of fields of prime characteristic.** Let E be an elementary abelian p-group of order $q = p^n$ and V a 2-dimensional faithful $\Bbbk E$-module. As every representation of a p-group is conjugate to one in upper-unitriangular form, we may fix a basis $\{X, Y\}$ of V such that the action of each $\alpha \in E$ is given by $\alpha \cdot X = X, \alpha \cdot Y = Y + \rho(\alpha)X$, where $\rho : E \to (\Bbbk, +)$ is a homomorphism, which must be injective as V is faithful. This allows us to regard E as an additive subgroup of $\Bbbk$ and prompts the study of such subgroups.

Lemma 3.2. *Let $G \leq \Bbbk$ be an additive subgroup. Define the polynomial*

$$T_G(x) = \prod_{\alpha \in G} (x - \alpha).$$

Then $T_G(x)$ is a linearized polynomial, i.e.

$$T_G(x) = \sum_{i=0}^{n} b_i x^{p^i}$$

for some coefficients $b_i \in \Bbbk$.

Proof. See [12, Theorem 3.52]. □

The author thanks Jyrki Lahtonen for bringing this lemma to his attention.

Corollary 3.3. *The power sum*

$$S_i(G) = \sum_{\alpha \in G} \alpha^i$$

is zero for all $i < q - 1$. Further, $S_{q-1}(G) \in \Bbbk$ is not zero.

Proof. We have $T_G(x) = \sum_{j=0}^{q} e_{q-j} x^j$ where e_j denotes the degree j elementary symmetric polynomial in the elements of G. For $j < q$, Lemma 3.2 implies that $e_j = 0$ unless $j = q - p^m$ for some $0 \leq m < n$. Now the power sums may be expressed in terms of elementary symmetric polynomials by means of the Newton-Girard identities; these are most readily written in matrix form as

$$S_i(G) = \begin{vmatrix} e_1 & 1 & 0 & \dots & 0 \\ 2e_2 & e_1 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ ie_i & e_{i-1} & e_{i-2} & \dots & e_1 \end{vmatrix}.$$

Now we see straight away that the leftmost column consists entirely of zeroes if $i < q - 1$, since for all $j \leq i$ we have either $e_j = 0$ or $j \equiv 0 \mod p$. We also see that $S_{q-1}(G) = -e_{q-1}$. Now e_{q-1} is equal to

$$\sum_{\beta \in G} \prod_{\alpha \in G, \alpha \neq \beta} \alpha.$$

But here the summands are all zero except when $\beta = 0$, hence

$$e_{q-1} = \prod_{\alpha \in G, \alpha \neq 0} \neq 0.$$

□

3.3. **Representations of elementary abelian p-groups.** For the rest of this section, let $E \leq \Bbbk$ and let $V = \langle X, Y\rangle$ be a 2-dimensional faithful $\Bbbk E$-module with action as in section 3.2. We want to study the modules $S^m(V)^*$. For any $i \leq m$ set $a_i = X^{m-i}Y^i$. Then the set $a_0, a_1, \ldots, a_m$ forms a basis of $S^m(V)$, and the action of $\alpha \in E$ on this basis is given by

$$\alpha \cdot a_i = \sum_{j=0}^{i} \binom{i}{j} \alpha^j a_{i-j}. \tag{2}$$

Notice that this does not depend on m; we have an inclusion $S^m(V) \subset S^{m+1}(V)$ for any $m \geq 0$. Now let $x_0, x_1 \ldots, x_m$ be the corresponding dual basis of $S^m(V)^*$; the action here is given by

$$\alpha \cdot x_i = \sum_{j=0}^{m-i} \binom{i+j}{i} (-\alpha)^j x_{i+j}. \tag{3}$$

Note in particular that $x_m \in (S^m(V)^*)^E$ and $S^m(V)^*/\langle x_m\rangle \cong S^{m-1}(V)^*$. This follows because $x_m = S^{m-1}(V)^\perp$. We adopt the convention that for a natural number r, rW denotes the direct sum of r copies of W.

Proposition 3.4. *The following is true of the modules $S^m(V)^*$:*

(i) *$S^m(V)^*$ is indecomposable for $m \leq q-1$, and $S^{q-1}(V)^* \cong \Bbbk E$.*
(ii) *$S^{qr+m}(V)^* \cong S^m(V)^* \oplus r\Bbbk E$ for $m \leq q-1$ and any r.*

Proof. By [3, Proposition 3.2], the ring of invariants $S(V)^E$ is a polynomial algebra generated by X and $N_E(Y)$. Therefore the Hilbert Series of $S(V)^E$ is

$$\frac{1}{(1-t)(1-t^q)}. \tag{4}$$

and so $\dim(S^m(V)^E) = 1$ for $m \leq q-1$. Since a module is indecomposable if and only if its dual is, and since $\dim(S^m(V)^*) = m+1$ we obtain (i).
Now let P denote the projective module $S^{q-1}(V)$, and let $B = \oplus_{i=0}^{q-2} S^i(V)$. We form the graded submodule $T = \bigoplus_{d\geq 0} T^d$ of $S(V)$ defined as

$$T = (\Bbbk[X, N_E(Y)] \otimes P) \oplus (\Bbbk[N_E(Y)] \otimes B), \tag{5}$$

with grading induced from that on $S(V)$. By Remark 3.1 , T is a direct summand of $S(V)$. Clearly $T^{qr+m} \cong r(\Bbbk E) \oplus S^m(V)$. The Hilbert series of $\Bbbk[N_E(Y)]$ is $\frac{1}{1-t^q}$. As the dimension of B in degree k is $k+1$ if $k \leq q-2$ and zero otherwise, we have

$$H(B,t) = 1 + 2t + 3t^2 + \ldots + (q-1)t^{q-2} = \frac{d}{dt}\left(\frac{1-t^q}{1-t}\right) = \frac{-qt^{q-1}}{1-t} + \frac{1-t^q}{(1-t)^2}.$$

Finally, as P has dimension q and lies in degree $q-1$, we have $H(P,t) = qt^{q-1}$. Therefore

$$H(T,t) = qt^{q-1}\frac{1}{(1-t)(1-t^q)} + \frac{1}{1-t^q}\left(\frac{-qt^{q-1}}{1-t} + \frac{1-t^q}{(1-t)^2}\right) = \frac{1}{(1-t)^2} = H(S(V),t).$$

Therefore $T = S(V)$. Taking duals on both sides gives the required result. □

We need a little more information about the decomposition above. Suppose that $0 \leq m < q$ and let $\{x_0, x_1, \ldots x_{qr+m}\}$ be a basis of $W = S^{qr+m}(V)^*$ such that the action of E on W is given by (3). Then we have

$$W/\langle x_{qr+m}\rangle \cong S^{qr+m-1} \cong \begin{cases} rS^{q-1}(V)^* \oplus (S^{m-1}(V)^*) & m \neq 0; \\ rS^{q-1}(V)^* & m = 0. \end{cases}$$

This tells us immediately that x_{qr+m} is contained in a summand of $S^{qr+m}(V)^*$ isomorphic to $S^m(V)^*$. Further, we observe that

Lemma 3.5. *The projective summand of W is spanned by*

$$\{\alpha \cdot x_{iq} : \alpha \in E, i = 0, \dots r-1.\}$$

Proof. Recall that for any p-group P an indecomposable $\Bbbk P$-module M is projective if and only if $\mathrm{Tr}^P(M) \neq 0$. Further, $\mathrm{Tr}^E(\Bbbk E)$ is one-dimensional. Now observe that for every $0 \leq i < r$ we have

$$\mathrm{Tr}^E(x_{iq}) = \sum_{j=0}^{m-iq} \binom{iq+j}{iq} \left(\sum_{\alpha \in E} (-\alpha)^j \right) x_{iq+j}$$

$$= \binom{iq+q-1}{iq} \left(\prod_{\alpha \in E, \alpha \neq 0} \alpha \right) x_{iq+q-1} + \text{lower degree terms}$$

by Corollary 3.3. The binomial coefficient here is equal to $1 \in \Bbbk$ by Lucas' Theorem (see [5]). Consequently $\mathrm{Tr}(x_{iq}) \neq 0$ and $\{\alpha \cdot x_{iq} : \alpha \in E\}$ spans a projective indecomposable summand of W for each i. □

Being projective, the modules $S^{q-1}(V)^*$ are permutation modules. It follows that their symmetric powers are also permutation modules. The next lemma helps identify the isomorphism classes of these permutation modules. For any $k \leq n$ we denote by $\mathcal{X}_k$ the set of subgroups of E with order $\leq p^k$.

Lemma 3.6. *Given $d > 0$ we write $d = rp^k$ where $k \leq n$ is maximal such that p^k divides d. Then we have*

(i) *If $k < n$, $S^d(\Bbbk E) \simeq_{\mathcal{X}_k} 0$.*
(ii) *If $k = n$ then $S^d(\Bbbk E) \simeq_{\mathcal{X}_{n-1}} \Bbbk$.*
(iii) *For any k we have more generally*

$$S^d(\Bbbk E) \simeq_{\mathcal{X}_{k-1}} \bigoplus_{E' \leq E, |E'| = p^k} \frac{1}{p^{n-k}} \binom{p^{n-k}+r-1}{r} \Bbbk \uparrow_{E'}^{E} .$$

Proof. Let W be a direct summand of $S^d(\Bbbk E)$. Then W is a permutation module; let $\{\sigma \cdot m : \sigma \in E\}$ be a basis of W, where m is some monomial of degree d. Then W has isomorphism type $\Bbbk \uparrow_{E'}^{E}$ where E' is the stabiliser of m. Clearly if the monomial m has stabiliser E' then m can be written as a product of monomials of the form $\prod_{\sigma \in E'}(\sigma m')$. In particular, we must have that $|E'|$ divides $\deg(m)$. This establishes (i). On the other hand, if $d = rp^n$ then there is a unique monomial with stabiliser E, namely $\prod_{\sigma \in E} x_\sigma^r$. This establishes (ii).

Now let E' be a subgroup of E with order p^k. Define a power series $P(E', t) = \sum_{d \geq 0} M_d^{E'} t^d$ where $M_d^{E'}$ is the number of monomials of degree d fixed by E'. Then we have

$$P(E', t) = \frac{1}{(1 - t^{p^k})^{p^{n-k}}}$$

$$= \sum_{r=0}^{\infty} \binom{p^{n-k}+r-1}{r} t^{rp^k}$$

by the generalised binomial theorem. Therefore the number of summands of $S^d(\Bbbk E)$ with isomorphism type $\Bbbk \uparrow_{E'}^{E}$ is $\frac{1}{p^{n-k}} \binom{p^{n-k}+r-1}{r}$, as each one spans a submodule of dimension p^{n-k}. As there are no trivial summands and all other summands are induced from smaller subgroups, we have proved (iii). □

3.4. **Main results.** In order to make the main results more readable we introduce some more notation: we write $B_{d,m}$ for $B^d(S^m(V)^*)$, and $\alpha_{d,m}$ for the map $S^d(S^m(V)^*) \to S^{d+1}(S^m(V)^*)$ described in section 3.1. By the remarks following equation 3 we obtain, for any d and $m < q$ an exact sequence

$$0 \longrightarrow B_{d,m} \xrightarrow{\alpha_{d,m}} B_{d+1,m} \longrightarrow B_{d+1,m-1} \longrightarrow 0. \tag{6}$$

When $E' < E$ is a proper subgroup we will write $B_{d,m}(E')$ for $B^d(S^m(V\downarrow_{E'})^*)$. Note that this is not the same thing as $B_{d,m}\downarrow_{E'}$; the former consists of polynomials whose degree as a polynomial in the terminal variable of $S^m(V)^*$ is $< |E'|$ while the latter consists of polynomials whose degree as a polynomial in the terminal variable of $S^m(V)^*$ is $< q$.

Proposition 3.7. *Let d, m be a pair of positive integers with $m < q$ and $m+d \geq q$. Then the following hold:*

(i) *$B_{d,m}$ is projective relative to the set of proper subgroups of E.*
(ii) *Assuming $n \geq 2$, let s and r be the quotients when d and m respectively are divided by p^{n-1}, with d' and m' the corresponding remainders. Then we have*

$$B_{d,m} \simeq_{\mathcal{X}_{n-2}} \bigoplus_{E'<E:|E'|=p^{n-1}} \frac{1}{p}\left[\binom{r+s}{r} - \binom{r+s-p}{r}\right] B_{d',m'}(E')\uparrow^E_{E'} \tag{7}$$

provided $\frac{1}{p}\left[\binom{r+s}{r} - \binom{r+s-p}{r}\right]$ is an integer, and

$$B_{d,m}(E) \simeq_{\mathcal{X}_{n-2}} 0$$

otherwise.

Remark 3.8. The proof is by double induction. The first induction is on n, the rank of E. We will show that the (i) above holds when $n = 1$. Then for the inductive step we will take a group E of order p^n and assume that both (i) and (ii) hold for all proper subgroups of E - although in the $n = 2$ case just (i) will be sufficient. We will then prove that (ii) holds for E. Notice that this implies immediately that (i) holds for E.

For each fixed n, we will prove (ii) by backwards induction on m, starting at $m = q-1$. This means we will initially prove that (ii) holds for all pairs $(d, q-1)$. Then in the inductive step we will fix $m \leq q-1$ and assume that (ii) holds for all pairs (d, m) such that $m+d \geq q$. We will prove (ii) holds for the pairs $(m-1, d+1)$. This part of the proof is the longest and relies on determining the equivalence class of the morphism $\alpha_{d,m} : B_{d,m} \to B_{d+1,m}$.

In various parts the proof splits into two or more subcases, depending on the value of d or m modulo $q' := p^{n-1}$. This will be made clear in the text.

Proof. **Initial step, $n = 1$.**
For the $n = 1$ case, only the first statement needs to be checked. This states that $B_{d,m}$ is projective provided $m+d \geq p$ and $m < p$. When $n = 1$, E is a cyclic group and the proposition reduces to Theorem 1.4; more precisely, to (i) when $d < p$ and to (ii) when $d \geq p$.
Inductive step for n.
Now fix $n > 1$, and assume that the proposition is true for all proper subgroups of E. The proof for each n is by downward induction on m, starting at $q-1$.

Initial step: $m = q-1$.
When $m = q-1$ we have $r = p-1$ and $m' = q'-1$. There are two cases to consider.

Case 1: $d' \neq 0$, i.e. d not divisible by q'.
Since $m' = q'-1$, we have $m'+d' \geq q'$. Therefore, for every subgroup $E' \leq E$ with

order q', $B_{d',m'}(E')$ is projective relative to $\mathcal{X}_{n-2}$ by the inductive hypothesis on n. Now the proposition becomes simply " $B_{d,q-1}$ is projective relative to $\mathcal{X}_{n-2}$". We showed that, when d is not divisible by q', $S^d(\Bbbk E)$ is projective relative to $\mathcal{X}_{n-2}$ in Lemma 3.6(iii). As $B_{d,q-1}$ is a direct summand of $S^d(S^{q-1}(V)^*)$ we get $B_{d,m} \simeq_{\mathcal{X}_{n-2}} 0$ as required.

Case 2: d' =0, i.e. d is divisible by q'.
In this case, $B_{d',m'}(E') = S^0(S^{q'-1}(V\downarrow_{E'})^*) = \Bbbk$. Furthermore since $d \geq p^{n-1}$ we have $s \geq 1$, hence $r+s \geq p$. So by Lemma 3.9

$$\binom{r+s}{r} \equiv \binom{r+s-p}{r} \mod p$$

and we have to show that,

$$B_{d,q-1} \simeq_{\mathcal{X}_{n-2}} \bigoplus_{E'<E:|E|=p^{n-1}} \frac{1}{p}\left[\binom{r+s}{r} - \binom{r+s-p}{r}\right] \Bbbk\uparrow^E_{E'}.$$

Now by Lemma 3.6(iii), we have

$$S^d(S^{q-1}(V)^*) \simeq_{\mathcal{X}_{n-2}} \bigoplus_{E'<E:|E|=p^{n-1}} \frac{1}{p}\binom{r+s}{r} \Bbbk\uparrow^E_{E'}$$

and $d-q = (s-p)p^{n-1}$ so

$$S^{d-q}(S^{q-1}(V)^*) \simeq_{\mathcal{X}_{n-2}} \bigoplus_{E'<E:|E|=p^{n-1}} \frac{1}{p}\binom{r+s-p}{r} \Bbbk\uparrow^E_{E'}$$

from which the result follows. This concludes the proof for $m = q-1$, and starts the induction on m.

Inductive step for m:
Now fix $m \leq q-1$ and assume that the proposition is true for all pairs of the form (d,m) such that and $m+d \geq q$. We must determine the equivalence class modulo $\mathcal{X}_{n-2}$ of $B_{d+1,m-1}$.

We have $B_{d+1,m-1} = \operatorname{coker}(\alpha_{d,m}|_{B_{d,m}})$. We use $\alpha_{d,m}$ for this map when the context is clear. We want to determine $B_{d+1,m-1}$ up to the addition of $\Bbbk E$-modules which are projective relative to $\mathcal{X}_{n-2}$; by Lemma 2.8 it is enough to compute $\operatorname{coker}(\alpha)$ where $\alpha \equiv_{\mathcal{X}_{n-2}} \alpha_{d,m}$.

Let the definitions of d', m', s, r be as in the statement of the proposition. We have several cases to consider.

Case 1: $d'+m' \geq q'$.
In this case $B_{d',m'}(E')$ is projective relative to $\mathcal{X}_{n-2}$ by the inductive hypothesis on n, and by the inductive hypothesis on m, $B_{d,m}$ is too. This is the domain of $\alpha_{d,m}$, which is injective, so we must have $\alpha_{d,m} \equiv_{\mathcal{X}_{n-2}} 0$. It follows that

$$B_{d+1,m-1} \simeq_{\mathcal{X}_{n-2}} B_{d+1,m}. \tag{8}$$

This case now splits into subcases. Let us denote by $(d+1)'$ the remainder when $d+1$ is divided by q'.

Subcase 1a: $d' \neq q'-1$.
In this case, $(d+1)' = d'+1$, and since $m'+d'+1 \geq m'+d' \geq q'$ we get $B_{d'+1,m'}(E') \simeq_{\mathcal{X}_{n-2}} 0$ by the inductive hypothesis (i) on n. Now by the inductive hypothesis (ii) on m we get that

$$B_{d+1,m} \simeq_{\mathcal{X}_{n-2}} 0.$$

So by (8) we get

$$B_{d+1,m-1} \simeq_{\mathcal{X}_{n-2}} 0$$

too.

This is exactly what the proposition claims in this subcase. Note that m' cannot be zero, since the assumption $m'+d' \geq q'$ then cannot hold. Therefore $(m-1)' = m'-1$, and since $(d+1)'+(m-1)' = d'+m' \geq q'$ we get $B_{d'+1,m'-1}(E') \simeq \mathcal{X}_{n-2}$ by the inductive hypothesis on n. Then the proposition (ii) states that

$$B_{d+1,m-1}(E') \simeq \mathcal{X}_{n-2}$$

which is what we have just shown.

Subcase 1b: $d' = q'-1$.

If $d' = q'-1$ then we have $(d+1)' = 0$. Further, the quotient when $d+1$ is divided by q' is then $s+1$. The assumption $m'+d' \geq q'$ rules out the possibility that $m' = 0$, so $(m-1)' = m'-1$ and the quotient when $m-1$ is divided by q' is still r. So the difference of binomial coefficients appearing in the formula (7) for $B_{d+1,m}$ is the same as the one appearing in the formula for $B_{d+1,m-1}$ and since

$$B_{(d+1)',(m-1)'}(E') = B_{0,m'-1}(E') = \Bbbk = B_{0,m'}(E') = B_{(d+1)',m'}$$

we get the desired equality. This ends the proof for case 1.

Case 2: $m'+d < q'$.

In this case, since $m+d \geq q$ we have

$$q \leq m+d = (r+s)p^{n-1} + m' + d'$$
$$\Rightarrow (r+s)p^{n-1} \geq q - m' - d' > p^n - p^{n-1} = p^{n-1}(p-1)$$

and therefore $r+s \geq p$. Since $m < q$ we get $r < p$ and by Lemma 3.9

$$\binom{r+s}{r} \equiv \binom{r+s-p}{r} \bmod p.$$

Therefore by the inductive hypothesis on m,

$$B_{d,m} \simeq_{\mathcal{X}_{n-2}} \bigoplus_{E'<E:|E'|=p^{n-1}} \frac{1}{p}\left[\binom{r+s}{r} - \binom{r+s-p}{r}\right] B_{d',m'}(E') \uparrow^E_{E'} .$$

Note that this is the domain of $\alpha_{d,m}$.

Claim:

$$\alpha_{d,m} \equiv_{\mathcal{X}_{n-2}} \alpha := \bigoplus_{E'<E:|E'|=p^{n-1}} \frac{1}{p}\left[\binom{r+s}{r} - \binom{r+s-p}{r}\right] \alpha_{d',m'}(E') \uparrow^E_{E'} . \quad (9)$$

Proof of claim: The inductive hypothesis on m implies that $B_{d,m}$ is projective relative to $\mathcal{X}_{n-1}$. Applying Corollary 2.7 with $\mathcal{X} = \mathcal{X}_{n-1}$ and $\mathcal{Y} = \mathcal{X}_{n-2}$ shows that it is enough to check that the formula (9) is correct on restriction to each $E' < E$ with $|E'| = p^{n-1}$. Now the Mackey formula implies that for any $\Bbbk E''$-module W we have

$$W \uparrow^E_{E''} \downarrow_{E'} \simeq_{\mathcal{X}_{n-2}} \begin{cases} 0 & E' \neq E'' \\ pW & E' = E''. \end{cases}$$

It follows that for any $E' < E$ with $|E'| = p^{n-1}$ we have

$$\alpha \downarrow_{E'} \simeq_{\mathcal{X}_{n-2}} \left[\binom{r+s}{r} - \binom{r+s-p}{r}\right] \alpha_{d',m'}(E').$$

On the other hand, as $\Bbbk E'$-modules $S^m(V)^* \cong S^{m'}(V)^* \oplus rS^{q'-1}(V)^*$ where $q' = p^{n-1}$. Following Proposition 3.4(ii), we take $\{x_0, x_{q'}, \ldots, x_{(r-1)q'}\}$ as the $\Bbbk E'$-module generators of the projective summand, and write

$$S^m(V)^* = \bigoplus_{i=0}^{r-1} (E' \cdot x_{iq'}) \oplus M$$

where M is the direct summand of $S^m(V)^*$ isomorphic to $S^{m'}(V)^*$. The map $\alpha_{d,m} \downarrow_{E'}$ is induced by multiplication by an element x of the fixed-point space of

M, such that the quotient of M by x is isomorphic to $S^{m'-1}(V)^*$ if $m' \neq 0$ and the zero module otherwise.

As $\Bbbk E'$-modules we have

$$S^d(S^m(V)^*) = \bigoplus_{i_1+i_2+\ldots+i_r+j=q's+d'} S^{i_1}(E'\cdot x_0)\otimes\ldots\otimes S^{i_r}(E'\cdot x_{(r-1)q'})\otimes S^j(M).$$

and

$$B^d(S^m(V)^*) = \bigoplus_{i_1+i_2+\ldots+i_r+j=q's+d'} S^{i_1}(E'\cdot x_0)_{\{<q\}}\otimes\ldots\otimes S^{i_r}(E'\cdot x_{(r-1)q'})\otimes S^j(M)$$

where $S^{i_1}(E\cdot x_0)_{\{<q\}}$ means polynomials of degree i_1 in the linear expressions $\{\sigma\cdot x_0 : \sigma\in E'\}$ whose degree as a polynomial in x_0 is $< q$. Since $\alpha_{d,m}\downarrow_{E'}$ is injective, we can ignore any modules in the decomposition of its domain which are projective relative to $\mathcal{X}_{n-2}$. Note that $S^*(E'\cdot x_{kq'})\simeq_{\mathcal{X}_{n-2}}\Bbbk[N_{E'}(x_{kq'})]$ by the proof of Lemma 3.6(ii). As $N_{E'}(x_0)$ has x_0-degree q' we have

$$S^*(E'\cdot x_0)_{\{<q\}}\simeq_{\mathcal{X}_{n-2}}\oplus_{i=0}^{p-1}\langle N_{E'}(x_0^i)\rangle.$$

So the domain $B_{d,m}(E)\downarrow_{E'}$ is equivalent to a summand of

$$\bigoplus_{j=0}^{s}\bigoplus_{\substack{i_1+i_2+\ldots+i_r=s-j\\ i_1<p}} N_{E'}(x_0^{i_1})\otimes\ldots\otimes N_{E'}(x_{(r-1)q'}^{i_r})\otimes S^{jq'+d'}(M).$$

Further, $S^{jq'+d'}(M)\cong S^{jq'+d'}(S^{m'}(V\downarrow_{E'})^*)\simeq_{\mathcal{X}_{n-2}} S^{d'}(S^{m'}(V)^*) = B_{d',m'}(E')$ by the inductive hypothesis on n, for all values of j. Therefore forgetting the grading we have

$$B_{d,m}(E)\downarrow_{E'}\simeq_{\mathcal{X}_{n-2}}\bigoplus_{j=0}^{s}\bigoplus_{\substack{i_1+i_2+\ldots+i_r=s-j\\ i_1<p}}\Bbbk\otimes\Bbbk\otimes\ldots\otimes\Bbbk\otimes B_{d',m'}(E') \tag{10}$$

and $\alpha_{d,m}\downarrow_{E'}$ on this is equivalent to

$$\bigoplus_{j=0}^{s}\bigoplus_{\substack{i_1+i_2+\ldots i_r=s-j\\ i_1<p}}(\mathrm{id}_\Bbbk\otimes\mathrm{id}_\Bbbk\ldots\otimes\mathrm{id}_\Bbbk\otimes\alpha_{d',m'}(E'))$$

Obviously all the summands appearing in (10) are isomorphic. The number of them is

$$\sum_{j=0}^{s}(\text{ Number of ways of writing } s-j \text{ as an ordered sum of } r \text{ non-negative integers, with the first} < p.\ ).$$

Let $\mathcal{P}(k,l)$ denote the number of ways of writing k as an ordered sum of l non-negative integers (where the order of summands is taken into account). An easy combinatorial argument shows that $\sum_{k=0}^{l}\mathcal{P}(k,l)=\binom{k+l}{k}$. Evidently the number of summands appearing in (10) is

$$\sum_{j=0}^{s}(\mathcal{P}(s-j,r)-\mathcal{P}(s-j-p,r)).$$

But clearly $\mathcal{P}(s-j-p,r)=0$ if $j>s-p$, so the number of summands is

$$\sum_{j=0}^{s}\mathcal{P}(s-j,r)-\sum_{j=0}^{s-p}\mathcal{P}(s-j-p,r)=\binom{r+s}{r}-\binom{r+s-p}{r}.$$

Now we have shown that

$$\alpha_{d,m}\downarrow_{E'}\simeq_{\mathcal{X}_{n-2}}\left[\binom{r+s}{r}-\binom{r+s-p}{r}\right]\alpha_{d',m'}(E')\equiv_{\mathcal{X}_{n-2}}\alpha\downarrow_{E'}$$

and hence $\alpha_{d,m}\equiv_{\mathcal{X}_{n-2}}\alpha$ which proves our claim.

Now we must show that the cokernel of $\alpha_{d,m}$ is given by the formula for $B_{d+1,m-1}$ in part (ii) of the proposition. Note that $\alpha_{d,m}$ has codomain $B_{d+1,m}$. There are three cases to check.

Subcase 2a: $m'\neq 0$**:** Note that in this case it is not possible to have $d'=q'-1$, since we must have $m'+d'<q'$. Therefore the quotients when m and $d+1$ are divided by q' are r and s respectively, and by the inductive hypothesis on m we have

$$B_{d+1,m}\simeq_{\mathcal{X}_{n-2}}\bigoplus_{E'<E:|E'|=p^{n-1}}\frac{1}{p}\left[\binom{r+s}{r}-\binom{r+s-p}{r}\right]B_{d'+1,m'}(E')\uparrow^E_{E'}$$

$$=\bigoplus_{E'<E:|E'|=p^{n-1}}\frac{1}{p}\left[\binom{r+s}{r}-\binom{r+s-p}{r}\right]\mathrm{codom}(\alpha_{d',m'}(E'))\uparrow^E_{E'} \tag{11}$$

and hence, using the formula (9) for α we have

$$B_{d+1,m-1}=\mathrm{coker}(\alpha_{d,m})\simeq_{\mathcal{X}_{n-2}}\bigoplus_{E'<E:|E'|=p^{n-1}}\frac{1}{p}\left[\binom{r+s}{r}-\binom{r+s-p}{r}\right]\mathrm{coker}(\alpha_{d',m'}(E'))\uparrow^E_{E'}$$

$$=\bigoplus_{E'<E:|E'|=p^{n-1}}\frac{1}{p}\left[\binom{r+s}{r}-\binom{r+s-p}{r}\right]B_{d'+1,m'-1}(E')\uparrow^E_{E'}$$

as required.

Subcase 2b: $m'=0,d'\neq q'-1$ On the other hand, if $m'=0$ then $\alpha_{d',m'}:\Bbbk\to\Bbbk$ is an isomorphism in $\mathcal{X}_{n-2}\,\mathrm{stmod}_{\Bbbk E'}$ for every subgroup $E'<E$ with order q'. If in addition $d'\neq q'-1$ then as the quotient when $d+1$ is divided by q' is still s, (11) still holds and

$$\mathrm{coker}\,\alpha_{d,m}\simeq_{\mathcal{X}_{n-2}}\bigoplus_{E'<E:|E'|=p^{n-1}}\frac{1}{p}\left[\binom{r+s}{r}-\binom{r+s-p}{r}\right]\mathrm{coker}(\alpha_{d',m'}(E'))\uparrow^E_{E'}$$

$$\simeq_{\mathcal{X}_{n-2}}0.$$

This is in agreement with (7) because $(m-1)'+(d+1)'=q'-1+d'+1\geq q'$, hence by the inductive hypothesis on n $B_{(d+1)',(m-1)'}\simeq_{\mathcal{X}_{n-2}}0$.

Subcase 2c: $m'=0,d'=q'-1$**.**
In this case, the quotient when $d+1$ is divided by q' is not s but $s+1$. We still have $r<p$ and $r+s+1\geq p$, so by Lemma 3.9 $\left[\binom{r+s+1}{r}-\binom{r+s+1-p}{r}\right]$ is divisible by p. Therefore by the inductive hypothesis on m we have

$$B_{d+1,m}\simeq_{\mathcal{X}_{n-2}}\bigoplus_{E'<E:|E'|=p^{n-1}}\frac{1}{p}\left[\binom{r+s+1}{r}-\binom{r+s+1-p}{r}\right]\Bbbk\uparrow^E_{E'}.$$

The map $\alpha_{d',m'}(E')$ is again an isomorphism for each $E'<E$ with order q', and so the image of α is contained in

$$\bigoplus_{E'<E:|E'|=p^{n-1}}\frac{1}{p}\left[\binom{r+s}{r}-\binom{r+s+p}{r}\right]\Bbbk\uparrow^E_{E'}.$$

Therefore the cokernel of $\alpha_{d,m}$ is

$$\simeq_{\mathcal{X}_{n-2}} \bigoplus_{E'<E:|E'|=p^{n-1}} \frac{1}{p}\left[\binom{r+s}{r-1} - \binom{r+s+p}{r-1}\right] \Bbbk \uparrow^E_{E'} .$$

This is what we want, because the quotient when $m-1$ is divided by q' is $r-1$ and the quotient when $d+1$ is divided by q' is $s+1$, so their sum is $r+s$, and $B_{(d+1)',(m-1)'} \simeq_{\mathcal{X}_{n-2}} B_{0,0} \cong \Bbbk$. □

In the above we used the following number-theoretic lemma:

Lemma 3.9. *Let r, s be integers and let p be a prime. Suppose that $r < p$ and $r+s \geq p$. Then*

$$\binom{r+s}{r} \equiv \binom{r+s-p}{r} \mod p$$

where the latter is interpreted as zero if $s < p$.

Proof. If $s < p$ then since $s + r \geq p$ we have

$$\binom{r+s}{r} = \frac{(r+s)(r+s-1)\cdots(p)\cdots(s+1)}{r(r-1)\cdots 2.1} \equiv 0 \mod p.$$

While if $s \geq p$ we have

$$\begin{aligned}\binom{r+s-p}{r} &= \frac{(r+s-p)(r+s-1-p)\cdots(s+1-p)}{r(r-1)\cdots 2\cdot 1} \\ &= \frac{(r+s)(r+s-1)\cdots(s+1)}{r(r-1)\cdots 2\cdot 1} \equiv \binom{r+s}{r} \mod p.\end{aligned}$$

□

The following Corollary contains both Theorems 1.5 and 1.6 as special cases.

Corollary 3.10. *Let (d, m) be a pair of positive integers, with $m < p^k \leq q$ and $m + d \geq q$. Then $B_{d,m}$ is projective relative to $\mathcal{X}_{k-1}$.*

Proof. The proof is by backwards induction on k, the case $k = n$ having been covered in Proposition 3.7. Let $k \leq l \leq n$ and assume that $B_{d,m}$ is projective relative to $\mathcal{X}_l$ for all pairs d, m with $d+m \geq q$ and $m < p^{l+1}$. Now suppose $m < p^l$ and $m+d \geq q$; we will show that $B_{d,m}$ is projective relative to $\mathcal{X}_{l-1}$. As $m < p^{l+1}$, we have that $B_{d,m}$ is projective relative to $\mathcal{X}_l$. So by Proposition 2.2(iv), $B_{d,m}$ is a direct summand of

$$\begin{aligned}&\bigoplus_{E'\in\mathcal{X}_l} (B_{d,m}\downarrow_{E'})\uparrow^E_{E'} \\ \simeq_{\mathcal{X}_{l-1}} &\bigoplus_{E'<E:|E'|=p^l} (B_{d,m}(E') \oplus B_{d-p^l,m}(E') \oplus \ldots \oplus B_{d-ap^l,m}(E'))\uparrow^E_{E'}\end{aligned}$$

where a is the largest integer such that $a \leq (p^{n-l}-1)$ and $d - ap^l \geq 0$. Note that

$$m + d - ap^l \geq m + d - p^l(p^{n-l}-1) = m + d - p^n + p^l \geq p^l,$$

therefore for each E' the modules $B_{d,m}(E'), B_{d-p^l,m}(E'), \ldots, B_{d-ap^l,m}(E')$ are projective relative to $\mathcal{X}_{l-1}$ by Proposition 3.7 applied to E', from which the result follows. □

4. Applications to invariant theory

Modular invariants of elementary abelian p-groups are a topic of much current interest in invariant theory - for example, [3] describes generating sets for all such algebras of invariants for representations of dimension 2, and in dimension 3 for groups of rank at most three. In this section we shall study the rings of invariants $\Bbbk[V]^E$ where E is an elementary abelian p-group of arbitary rank, $\Bbbk$ is an infinite field of characteristic p and $V \cong S^{m_1}(W) \oplus \ldots \oplus S^{m_r}(W)$ for some faithful indecomposable $\Bbbk E$-module W of dimension two, and for some set of integers $m_1, m_2, \ldots, m_r$ with $1 \leq m_i < q$ for all i. (We assume $m_i \geq 1$ for each, as clearly $\Bbbk[V \oplus \Bbbk]^G = \Bbbk[V]^G \otimes \Bbbk[x]$ where x generates the trivial summand). Let k be the smallest integer such that $m_i < p^k$ for all i. We view E as an additive subgroup of $\Bbbk$ as in section 3.2. Let $x_{0,1}, x_{1,1}, \ldots x_{m_r,r}$ be the basis of V^* such that the action of $\alpha \in E$ on $\{x_{0,i}, \ldots, x_{m_i,i}\}$ is given by the formula (3) for all i, and let

$$N_i = N_E(x_{0,i}) = \prod_{\alpha \in E} \alpha \cdot (x_{0,i}).$$

If $f \in \Bbbk[V]$ then we shall say that f is of multidegree $(d_1, d_2, \ldots, d_r)$ if f has degree d_i in $\{x_{0,i}, \ldots, x_{m_i,i}\}$ for all i. We have a decomposition

$$\Bbbk[V]_{d_1,d_2,\ldots,d_r} \cong \Bbbk[S^{m_1}(W)]_{d_1} \otimes \Bbbk[S^{m_2}(W)]_{d_2} \otimes \ldots \otimes \Bbbk[S^{m_r}(W)]_{d_r}.$$

Further, for each i where $d_i \geq q$ we have $\Bbbk[S^{m_i}(W)]_{d_i} \cong S^{d_i}(S^{m_i}(W)^*) \cong N_i^{s_i} \otimes S^{d_i'}(S^{m_i}(W)^*) \oplus B_{d_i,m_i}$ where d_i' and s_i are the remainder and quotient when d_i is divided by q and B_{d_i,m_i} is the set of polynomials in $S^{d_i}(S^{m_i}(W)^*)$ whose degree in $x_{0,i}$ is $< q$. Notice that, by Corollary 3.10, B_{d_i,m_i} is projective relative to $\mathcal{X}_{k-1}$, if $d_i \geq q - m_i$.

Proposition 4.1. *$\Bbbk[V]^E$ has a generating set consisting of*

(i) *The orbit products N_i, $i = 1, \ldots, r$;*
(ii) *Certain invariants of multidegree $(d_1, d_2, \ldots, d_r)$, where $d_i < q - m_i$ for all i.*
(iii) *Certain invariants of the form $\mathrm{Tr}_H^E(f)$ for $f \in \Bbbk[V]^H$, where $H \in \mathcal{X}_{k-1}$.*

Proof. Let $f \in \Bbbk[V]^E_{d_1,d_2,d_3,\ldots,d_r}$. If $d_i < q - m_i$ for all i there is nothing to prove. If for some i we have $q - m_i \leq d_i < q$ then

$$\Bbbk[V]^E_{d_1,d_2,d_3,\ldots,d_r} \cong \Bbbk[S^{m_1}(W)]_{d_1} \otimes \Bbbk[S^{m_2}(W)]_{d_2} \otimes \ldots \otimes \Bbbk[S^{m_i}(W)]_{d_i} \otimes \ldots \otimes \Bbbk[S^{m_r}(W)]_{d_r}$$

is projective relative to $\mathcal{X}_{k-1}$ by the above discussion and Corollary 2.3. Then by Lemma 2.9 we have $f \in I^E_{\mathcal{X}_{k-1}}$. This completes the proof in case $d_i < q$ for all i. So now assume that $d_i \geq q$. The proof is now by induction on the total degree of f (the case of total degree $< q$ being settled already). We can write

$$f = N_i^{s_i} f' + b$$

for some unique $f' \in \Bbbk[V]_{d_1,d_2,\ldots,d_i',\ldots,d_r}$ and $b \in \Bbbk[V]_{d_1,d_2,\ldots,d_i,\ldots,d_r}$ whose degree in $x_{0,i}$ is $< q$. Furthermore for any $\alpha \in E$ we have

$$f = \alpha \cdot f = N_i^{s_i}(\alpha \cdot f') + \alpha \cdot b$$

so the uniqueness of division with remainder implies that f' and b are invariant. By induction, f' belongs to the subalgebra of $\Bbbk[V]^E$ generated by the claimed generating set and b is a fixed point in

$$\Bbbk[S^{m_1}(W)]_{d_1} \otimes \ldots \otimes \Bbbk[S^{m_{i-1}}(W)]_{d_{i-1}} \otimes B_{d_i,m_i} \otimes \Bbbk[S^{m_{i+1}}(W)]_{d_{i+1}} \otimes \ldots \otimes \Bbbk[S^{m_r}(W)]_{d_r}$$

which, by Corollary 2.3 and Theorem 3.10 is projective relative to $\mathcal{X}_{k-1}$. Then by Lemma 2.9 we have $b \in I^E_{\mathcal{X}_{k-1}}$. This completes the proof. □

In the case $q = p$ the above result is due to Wehlau [18], who also obtains more information about the invariants of type (ii) appearing in the generating set. Note that, since for a cyclic group E of order p every $\Bbbk E$-module can be decomposed into one of the form $S^{m_1}(W) \oplus \ldots \oplus S^{m_r}(W)$ with W the unique indecomposable of dimension 2, Wehlau's result applies to all modular representations of cyclic groups of prime order. Contrastingly, we do not know whether Proposition 4.1 can be generalised to arbitrary modular representations of elementary abelian p-groups.

In the case $r = 1$ we obtain

Proposition 4.2. *Let $m < p^k \leq q$ and let $\mathcal{X}$ be the set of subgroups of E with order $< p^k$. Let $V = S^m(W)$. Then the quotient algebra $\Bbbk[V]^E/I^E_{\mathcal{X}}$ is generated by images of invariants of degree at most q.*

Taking $k = n$ above in particular implies Theorem 1.3.

4.1. **Coinvariants and degree bounds.** Let G be a finite group of order divisible by p and V a finite-dimensional $\Bbbk$-vector space. The Hilbert Ideal $\mathcal{H}$ of $\Bbbk[V]$ is defined to be the ideal generated by positive degree invariants, i.e. $\Bbbk[V]^G_+\Bbbk[V]$. The algebra of coinvariants $\Bbbk[V]_G$ is defined to be the quotient $\Bbbk[V]^G/\mathcal{H}$, or equivalently as $\Bbbk[V] \otimes_{\Bbbk[V]^G} \Bbbk$. This is a finite-dimensional $\Bbbk G$-module.

Since the map Tr^G is $\Bbbk[V]^G$-linear, it follows that Tr^G maps a vector space basis for $\Bbbk[V]_G$ to a generating set of the ideal I^G_1. This observation was used to compute the Noether numbers for arbitary modular representations of cyclic groups of order p in [6, Corollary 3.4]. We want a similar result for elementary abelian p-groups.

We use the notation of the previous subsection, so let E be an elementary abelian p-group of order $q = p^n$, and W a faithful indecomposable $\Bbbk E$-module of dimension 2. Let $V = S^{m_1}(W) \oplus \ldots \oplus S^{m_r}(W)$, where $1 \leq m_i < p$ for all $i = 1, \ldots, r$. Recall that we may identify E with a subgroup of $\Bbbk$ and choose a basis $x_{0,1}, x_{1,1}, \ldots x_{m_r,r}$ of V^* such that the action of $\alpha \in E$ is given by the formula (3). Recall that $\{x_{1,1}, x_{2,1}, \ldots, x_{m_1,1}, \ldots, x_{m_r,r}\}$ is a $\Bbbk E$-submodule of V^*, and let A be the $\Bbbk G$-subalgebra of $S(V^*)$ generated by these variables. We use a graded lexicographic order on $S(V^*)$ with $x_{m_i,i} < x_{m_i-1,i} < \ldots < x_{0,i}$ for all i.

Proposition 4.3. *Let m be a monomial of degree $q-1$ in A. Then m is the lead term of an element of $\mathcal{H}$.*

Proof. Write $m = \prod_{j=1}^{q-1} u_j$ where for each j we have $u_j = x_{i(j),t(j)}$ for some $t(j) = 1, \ldots, r$ and $i(j) = 1, \ldots, m_{t(j)}$. For each j we define $u'_j = x_{i(j)-1,t(j)}$, and write $m' = \prod_{j=1}^{q-1} u'_j$. Now for each $S \subseteq \{1, 2, \ldots, q-1\}$ we define $S' := \{1, 2, 3, \ldots, q-1\} \backslash S$ and $X_S := \prod_{j \in S} u'_j$. Now define

$$F = \sum_{\alpha \in E} \prod_{j=1}^{q-1} (u'_j - \alpha \cdot u'_j).$$

On the one hand, we have

$$\prod_{j=1}^{q-1} (u'_j - \alpha \cdot u'_j) = \prod_{S \subseteq \{1,2,\ldots,q-1\}} (-1)^{|S|} X_S (\alpha \cdot X_{S'}).$$

Therefore

$$F = \prod_{S \subseteq \{1,2,\ldots,q-1\}} (-1)^{|S|} X_S \, \mathrm{Tr}^E(X_{S'})$$

which shows that $F \in \mathcal{H}$. Note that

$$\alpha \cdot u'_j = \alpha \cdot x_{i(j)-1,t(j)} = x_{i(j)-1,t(j)} - \alpha i(j) x_{i(j),t(j)} + \text{terms of lower degree.}$$

Since $m_t < p$ for all $t = 1, \dots, r$, the integer $i(j)$ is not zero in $\Bbbk$. It follows that the lead term of $u'_j - \alpha \cdot u'_j$ is $-\alpha i(j) u_j$. Therefore the lead term of F is $\sum_{\alpha \in E} (-\alpha)^{q-1} \lambda m$, where $\lambda = \prod_{j=1}^{q-1} i(j)$ is a non-zero element of $\mathbb{F}_p \subset \Bbbk$. By Corollary 3.3, $\sum_{\alpha \in E} (-\alpha)^{q-1} = \mu$ is a nonzero element of $\Bbbk$ and hence the lead term of F is $\mu\lambda m$. Dividing F by $\mu\lambda$ then produces an element of $\mathcal{H}$ with lead term m. □

Corollary 4.4. *The top degree of the coinvariants $\Bbbk[V]_E$ is bounded above by $q - 2 + r(q-1)$.*

Proof. It is well known that, with respect to any graded ordering of variables, the Hilbert series of a graded ideal and its ideal of lead terms coincide. Therefore it suffices to prove that any monomial of degree $> q - 2 + r(q-1)$ must be the lead term of an element of the Hilbert ideal. Let $m \in \Bbbk[V]$ be a monomial which is not the lead term of an element of $\mathcal{H}$. Write $m = \prod_{i=1}^{r} x_{0,i}^{k_i} h$ where $h \in A$. By Proposition 4.3, $\deg(h) \leq q - 2$. Further, since $x_{0,i}^q$ is the lead term of $N_E(x_{0,i})$ we must have $k_i \leq q - 1$ for each $i = 1, \dots, r$. This completes the proof. □

The case $r = 1$ of the following Corollary is Theorem 1.1.

Corollary 4.5. *The Noether number $\beta(\Bbbk[V]^E)$ is bounded above by $q - 2 + r(q-1)$.*

Proof. Proposition 4.1 with $k = 1$ implies that $\Bbbk[V]^E$ is generated by the orbit products $N_1, N_2, \dots, N_r$ which have degree q, certain invariants of (total) degree $\leq rq - \sum_{i=1}^{r} (m_i + 1) \leq r(q-2)$, and elements of I_1^E. Now the previous Corollary implies $\Bbbk[V]_E$ has a vector space basis $f_0, f_1, \dots, f_l$ consisting of polynomials of degree $\leq q - 2 + r(q-1)$. Therefore I_1^E is generated as a $\Bbbk[V]^E$ module by $\mathrm{Tr}^E(f_0), \mathrm{Tr}^E(f_1), \dots, \mathrm{Tr}^E(f_l)$. The result now follows by induction on degree. □

Note that we need the condition $m_i < p$ for all i, otherwise the generating set provided by Proposition 4.1 may contain elements of the form $\mathrm{Tr}_H^E(f)$ for non-trivial subgroups H of E. It is fairly straightforward to show that the degrees of these transfers are bounded above by the top degree of the *relative coinvariants* ${}_H\Bbbk[V]_E := \Bbbk[V] \otimes_{\Bbbk[V]^E} \Bbbk[V]^H$, but we do not know a method of obtaining an upper bound for this at present.

References

[1] Gert Almkvist and Robert Fossum. Decomposition of exterior and symmetric powers of indecomposable $\mathbf{Z}/p\mathbf{Z}$-modules in characteristic p and relations to invariants. In *Séminaire d'Algèbre Paul Dubreil, 30ème année (Paris, 1976–1977)*, volume 641 of *Lecture Notes in Math.*, pages 1–111. Springer, Berlin, 1978.

[2] D. J. Benson. *Representations and cohomology. I*, volume 30 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, second edition, 1998. Basic representation theory of finite groups and associative algebras.

[3] H. E. A. Campbell, R. J. Shank, and D. L. Wehlau. Rings of invariants for modular representations of elementary abelian p-groups. *Transform. Groups*, 18(1):1–22, 2013.

[4] Jon F. Carlson. *Modules and group algebras*. Lectures in Mathematics ETH Zürich. Birkhäuser Verlag, Basel, 1996. Notes by Ruedi Suter.

[5] N. J. Fine. Binomial coefficients modulo a prime. *Amer. Math. Monthly*, 54:589–592, 1947.

[6] P. Fleischmann, M. Sezer, R. J. Shank, and C. F. Woodcock. The Noether numbers for cyclic groups of prime order. *Adv. Math.*, 207(1):149–155, 2006.

[7] Peter Fleischmann. Relative trace ideals and Cohen-Macaulay quotients of modular invariant rings. In *Computational methods for representations of groups and algebras (Essen, 1997)*, volume 173 of *Progr. Math.*, pages 211–233. Birkhäuser, Basel, 1999.

[8] Peter Fleischmann. The Noether bound in invariant theory of finite groups. *Adv. Math.*, 156(1):23–32, 2000.

[9] John Fogarty. On Noether's bound for polynomial invariants of a finite group. *Electron. Res. Announc. Amer. Math. Soc.*, 7:5–7 (electronic), 2001.

[10] Frank Himstedt and Peter Symonds. Exterior and symmetric powers of modules for cyclic 2-groups. *J. Algebra*, 410:393–420, 2014.
[11] Ian Hughes and Gregor Kemper. Symmetric powers of modular representations, Hilbert series and degree bounds. *Comm. Algebra*, 28(4):2059–2088, 2000.
[12] Rudolf Lidl and Harald Niederreiter. *Introduction to finite fields and their applications*. Cambridge University Press, Cambridge, first edition, 1994.
[13] Amnon Neeman. *Triangulated categories*, volume 148 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 2001.
[14] Peter Symonds. Cyclic group actions on polynomial rings. *Bull. Lond. Math. Soc.*, 39(2):181–188, 2007.
[15] Peter Symonds. On the Castelnuovo-Mumford regularity of rings of polynomial invariants. *Ann. of Math. (2)*, 174(1):499–517, 2011.
[16] Burt Totaro. *Group cohomology and algebraic cycles*, volume 204 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 2014.
[17] D. L. Wehlau. Some problems in invariant theory. In *Invariant theory in all characteristics*, volume 35 of *CRM Proc. Lecture Notes*, pages 265–274. Amer. Math. Soc., Providence, RI, 2004.
[18] David L. Wehlau. Invariants for the modular cyclic group of prime order via classical invariant theory. *J. Eur. Math. Soc. (JEMS)*, 15(3):775–803, 2013.

Middlesex University, The Burroughs, London, NW4 4BT
E-mail address: j.elmer@mdx.ac.uk